

WHAT IS CLAIMED IS:

1. A method of generating an authentication ciphering offset (ACO) in a communication device, the method comprising:

generating the ACO as a function of one or more parameters, wherein at
5 least one of the one or more parameters is derived from earlier-computed values of the ACO.

2. The method of claim 1, wherein the step of generating the ACO as a function of one or more parameters comprises generating a k th value, X_k from one or more of the parameters, and applying a commutative binary operation between
10 X_k and a previous value, ACO_{k-1} .

3. The method of claim 1, wherein the step of generating the ACO as a function of one or more parameters comprises:

generating a k th value of ACO as a running sum in accordance with:

$$ACO_k = X_k \oplus ACO_{k-1} = \sum_{i=1}^k X_i ,$$

wherein X_i is generated as a function of the one or more parameters excluding the
15 at least one of the one or more parameters that is derived from earlier-computed values of the ACO.

4. The method of claim 3, wherein the sum is a bitwise modulo-2 sum.

5. The method of claim 4, wherein the bitwise modulo-2 sum is performed by means of a bitwise exclusive-OR (XOR) operation.

6. An apparatus for generating an authentication ciphering offset (ACO) in a communication device, the apparatus comprising:

logic configured to generate the ACO as a function of one or more parameters,

5 wherein at least one of the one or more parameters is derived from earlier-computed values of the ACO.

7. The apparatus of claim 6, wherein the logic configured to generate the ACO as a function of one or more parameters comprises logic configured to generate a k th value, X_k from one or more of the parameters, and to apply a commutative binary operation between X_k and a previous value, ACO_{k-1} .

8. The apparatus of claim 6, wherein the logic configured to generate the ACO as a function of one or more parameters comprises:

logic configured to generate a k th value of ACO as a running sum in accordance with:

$$ACO_k = X_k \oplus ACO_{k-1} = \sum_{i=1}^k X_i,$$

15 wherein X_i is generated as a function of the one or more parameters excluding the at least one of the one or more parameters that is derived from earlier-computed values of the ACO.

9. The apparatus of claim 8, wherein the logic configured to generate a k th value of ACO comprises logic configured to perform a bitwise modulo-2 sum.

5

12. The apparatus of claim 6, wherein the communication device includes a non-real-time device.

Year	1960	1961	1962	1963	1964	1965	1966	1967	1968	1969	1970	1971	1972	1973	1974	1975	1976	1977	1978	1979	1980	1981	1982	1983	1984	1985	1986	1987	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	2037	2038	2039	2040	2041	2042	2043	2044	2045	2046	2047	2048	2049	2050	2051	2052	2053	2054	2055	2056	2057	2058	2059	2060	2061	2062	2063	2064	2065	2066	2067	2068	2069	2070	2071	2072	2073	2074	2075	2076	2077	2078	2079	2080	2081	2082	2083	2084	2085	2086	2087	2088	2089	2090	2091	2092	2093	2094	2095	2096	2097	2098	2099	2100
1960	1961	1962	1963	1964	1965	1966	1967	1968	1969	1970	1971	1972	1973	1974	1975	1976	1977	1978	1979	1980	1981	1982	1983	1984	1985	1986	1987	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035	2036	2037	2038	2039	2040	2041	2042	2043	2044	2045	2046	2047	2048	2049	2050	2051	2052	2053	2054	2055	2056	2057	2058	2059	2060	2061	2062	2063	2064	2065	2066	2067	2068	2069	2070	2071	2072	2073	2074	2075	2076	2077	2078	2079	2080	2081	2082	2083	2084	2085	2086	2087	2088	2089	2090	2091	2092	2093	2094	2095	2096	2097	2098	2099	2100	